ASA 8.x/ASDM 6.x: Agregue la nueva información de peer VPN en un VPN de sitio a sitio existente usando el ASDM

Contenido

Introducción

Este documento proporciona la información sobre los cambios basados en la configuración para hacer cuando agregan a un nuevo par VPN a la configuración existente del VPN de sitio a sitio usando el Administrador de dispositivos de seguridad adaptante (ASDM). Esto se requiere en estos escenarios:

- Se ha cambiado el Proveedor de servicios de Internet (ISP) y un nuevo conjunto de intervalo de direcciones IP público se utiliza.
- Un reajuste completo de la red en un sitio.
- El dispositivo usado como gateway de VPN en un sitio se emigra a un nuevo dispositivo con un diverso IP Address público.

Este documento asume que el VPN de sitio a sitio está configurado ya correctamente y trabaja muy bien. Este documento proporciona los pasos para seguir para cambiar una información de peer VPN en la configuración VPN L2L.

prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de este tema:

- Ejemplo de configuración del VPN de sitio a sitio ASA

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 5500 Series del dispositivo de seguridad de Cisco Adapative con la versión de software 8.2 y posterior
- Administrador de dispositivos de seguridad de Cisco Adapative con la versión de software 6.3 y posterior

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Información de Backround

El VPN de sitio a sitio está trabajando muy bien entre el HQASA y el BQASA. Asuma que el BQASA tiene un reajuste completo de la red y el esquema IP se ha modificado en el nivel ISP, pero todos los detalles internos del red secundario siguen siendo lo mismo.

Esta configuración de muestra utiliza estos IP Addresses:

- IP Address externo existente BQASA - 200.200.200.200
- Nuevo IP Address externo BQASA - 209.165.201.2

Nota: Aquí, solamente la información de peer será modificada. Porque no hay otro cambio en la subred interna, las listas de acceso crypto siguen siendo lo mismo.

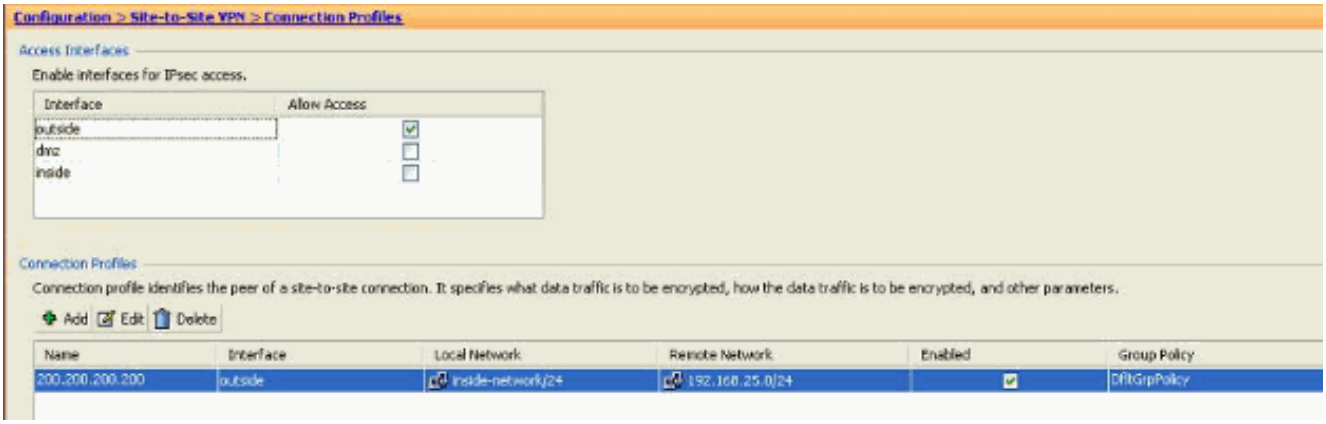
Configuración de ASDM

Esta sección proporciona la información sobre los métodos posibles usados para cambiar la información de peer VPN en HQASA usando el ASDM.

Cree un perfil de la nueva conexión

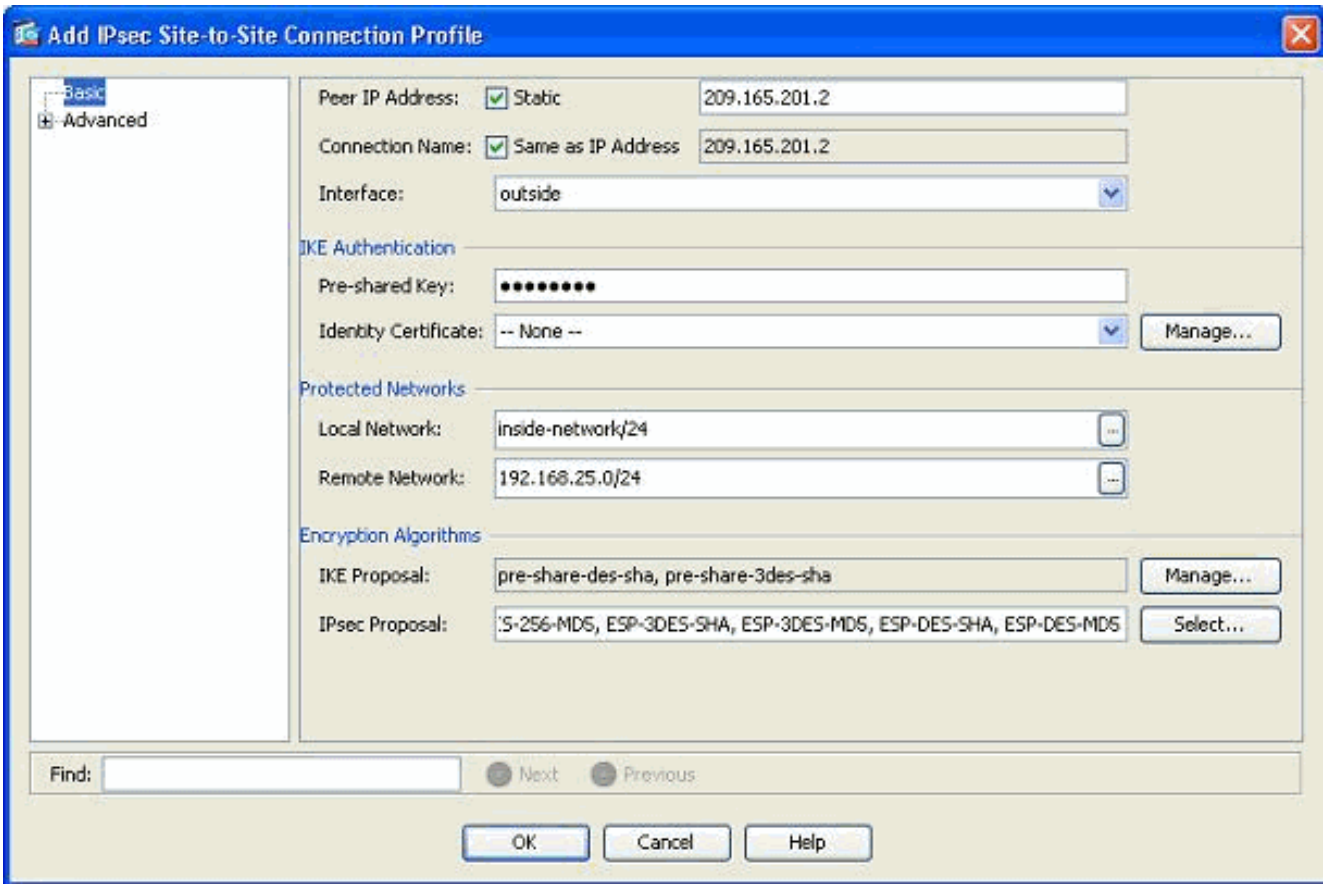
Éste puede ser el método más fácil porque no perturba la configuración VPN existente y puede crear un perfil de la nueva conexión con la nueva información relacionada del par VPN.

1. Vaya a la *configuración > al VPN de sitio a sitio > a los perfiles de la conexión* y el tecleo *agrega* bajo área de los perfiles de la conexión.

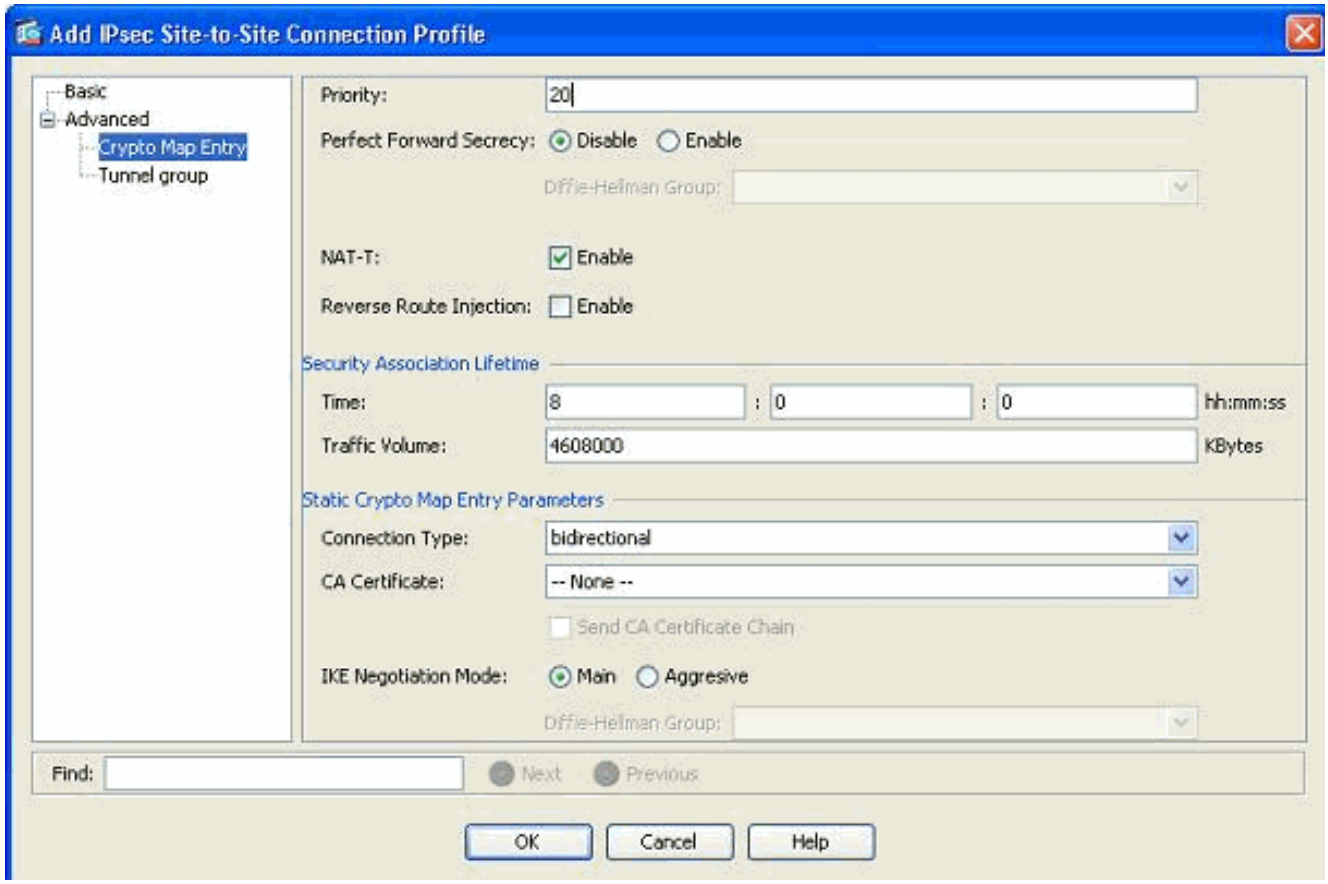


La ventana del *perfil de la conexión del sitio a localizar del IPSec del agregar* abre.

2. Bajo lengueta básica, proporcione los detalles para el *IP Address de Peer*, la *clave previamente compartida*, y las *redes protegidas*. Utilice aun así los parámetros como el VPN existente, excepto la información de peer. Haga clic en
OK.



3. Bajo menú avanzado, *entrada de correspondencia de criptografía del* tecleo. Refiera a la lengueta de la *prioridad*. Esta prioridad es igual al número de secuencia en su configuración CLI equivalente. Cuando un poco número que la entrada de correspondencia de criptografía existente se asigna, este nuevo perfil se ejecuta primero. Cuanto más alto es el número de prioridad, menos el valor. Esto se utiliza para cambiar la orden de la secuencia que una correspondencia de criptografía específica será ejecutada. Haga Click en OK a completar creando el perfil de la nueva
conexión.



Esto crea automáticamente a un nuevo grupo de túnel junto con una correspondencia de criptografía asociada. Aseegurese le puede alcanzar el BQASA con la nueva dirección IP antes de que usted utilice este perfil de la nueva conexión.

Edite la configuración VPN existente

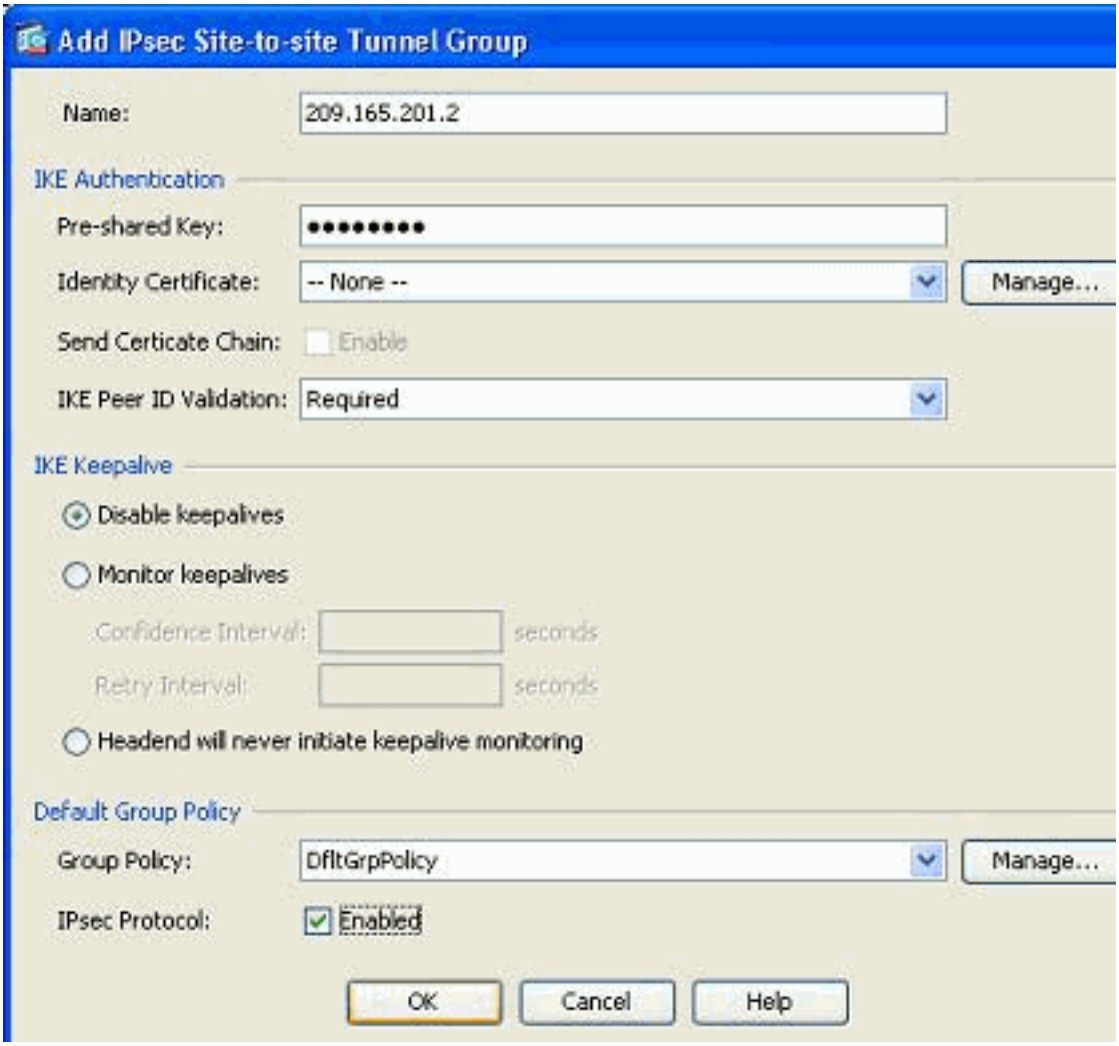
Otra manera de agregar a un nuevo par es modificar la configuración existente. El perfil de la conexión existente no se puede editar para la nueva información de peer porque está limitado a un par específico. Para editar la configuración existente, usted necesita realizar estos pasos:

1. Cree a un nuevo grupo de túnel
2. Edite la correspondencia de criptografía existente

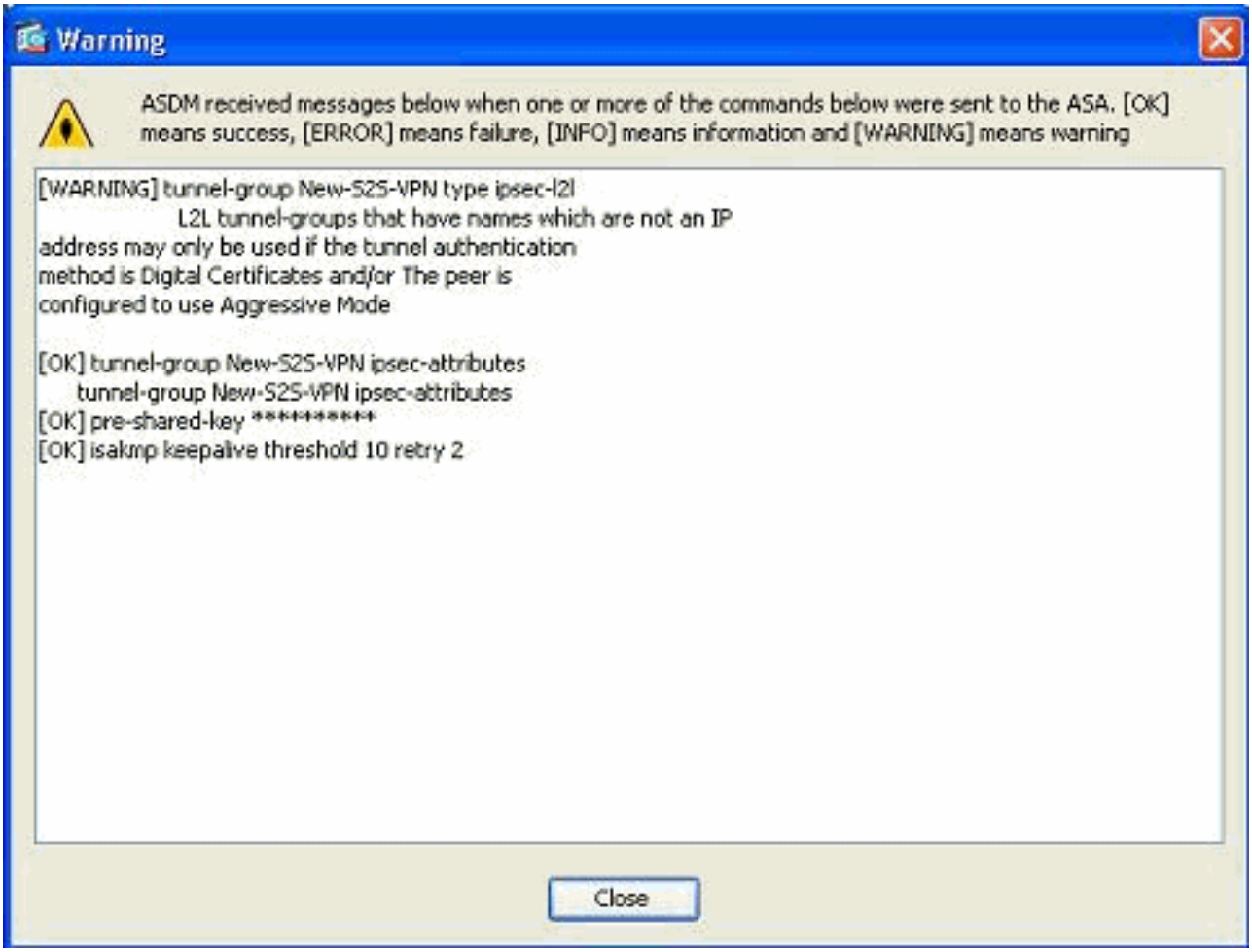
Cree a un nuevo grupo de túnel

Van a la *configuración > al VPN de sitio a sitio > avanzaron > los grupos de túnel* y el tecleo *agrega* para crear a un nuevo grupo de túnel que contenga la nueva información de peer VPN. Especifique los campos del *nombre* y de *clave previamente compartida*, después haga clic la *AUTORIZACIÓN*.

Nota: Aseegurese la clave previamente compartida hace juego el otro extremo del VPN.



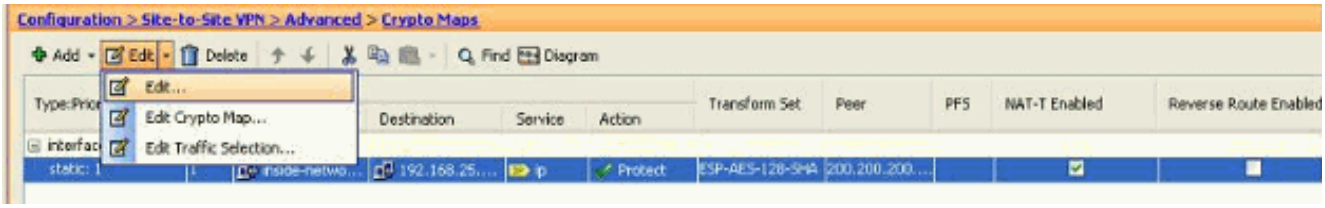
Nota: En el campo de nombre, solamente el IP Address del peer remoto debe ser ingresado cuando el modo de autenticación es claves previamente compartidas. Cualquier nombre puede ser utilizado solamente cuando el método de autentificación está a través de los Certificados. Este error aparece cuando un nombre se agrega en el campo de nombre y PRE-se comparte el método de autentificación:



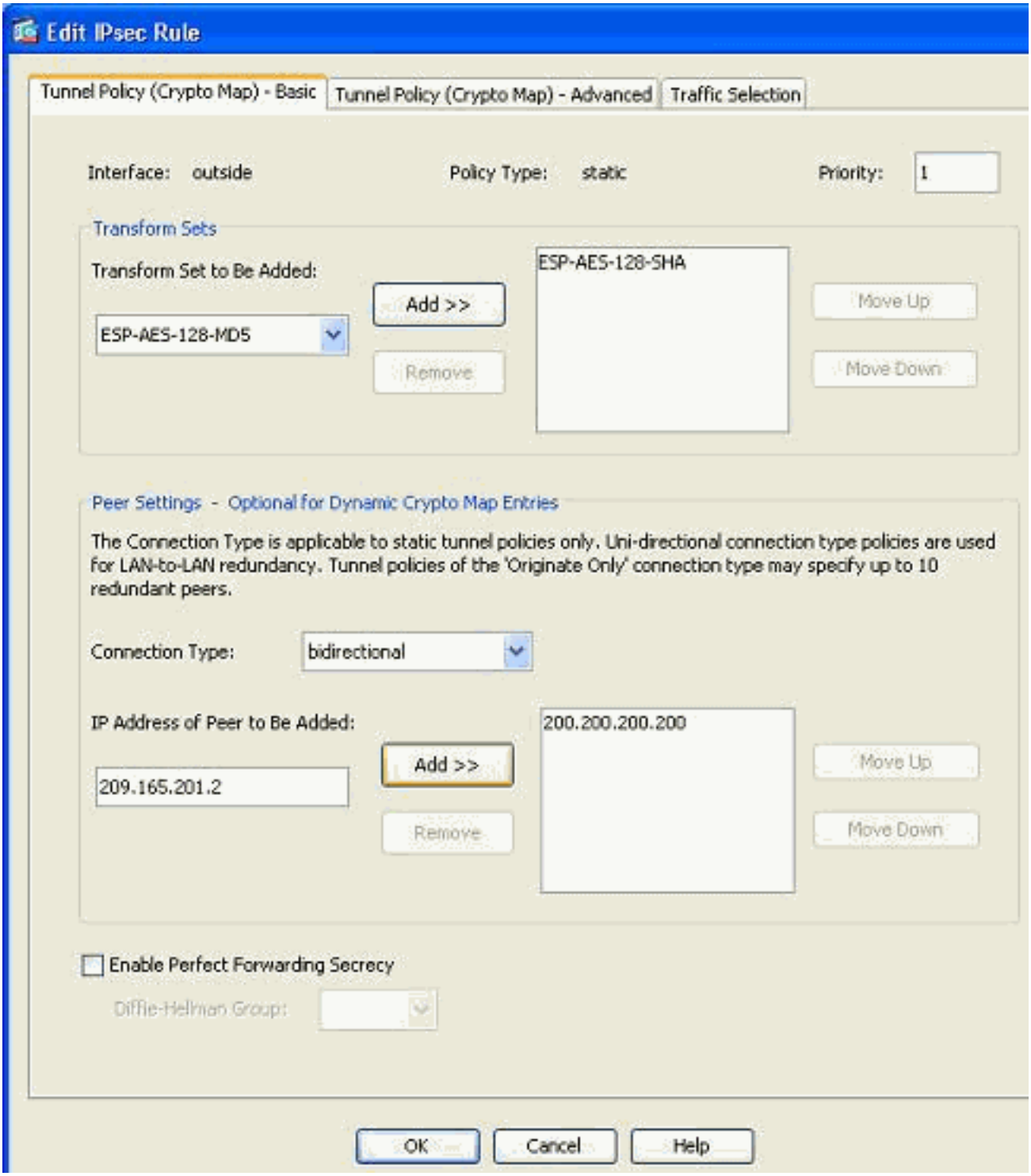
Edite la correspondencia de criptografía existente

La correspondencia de criptografía existente se puede editar para asociar la nueva información de peer.

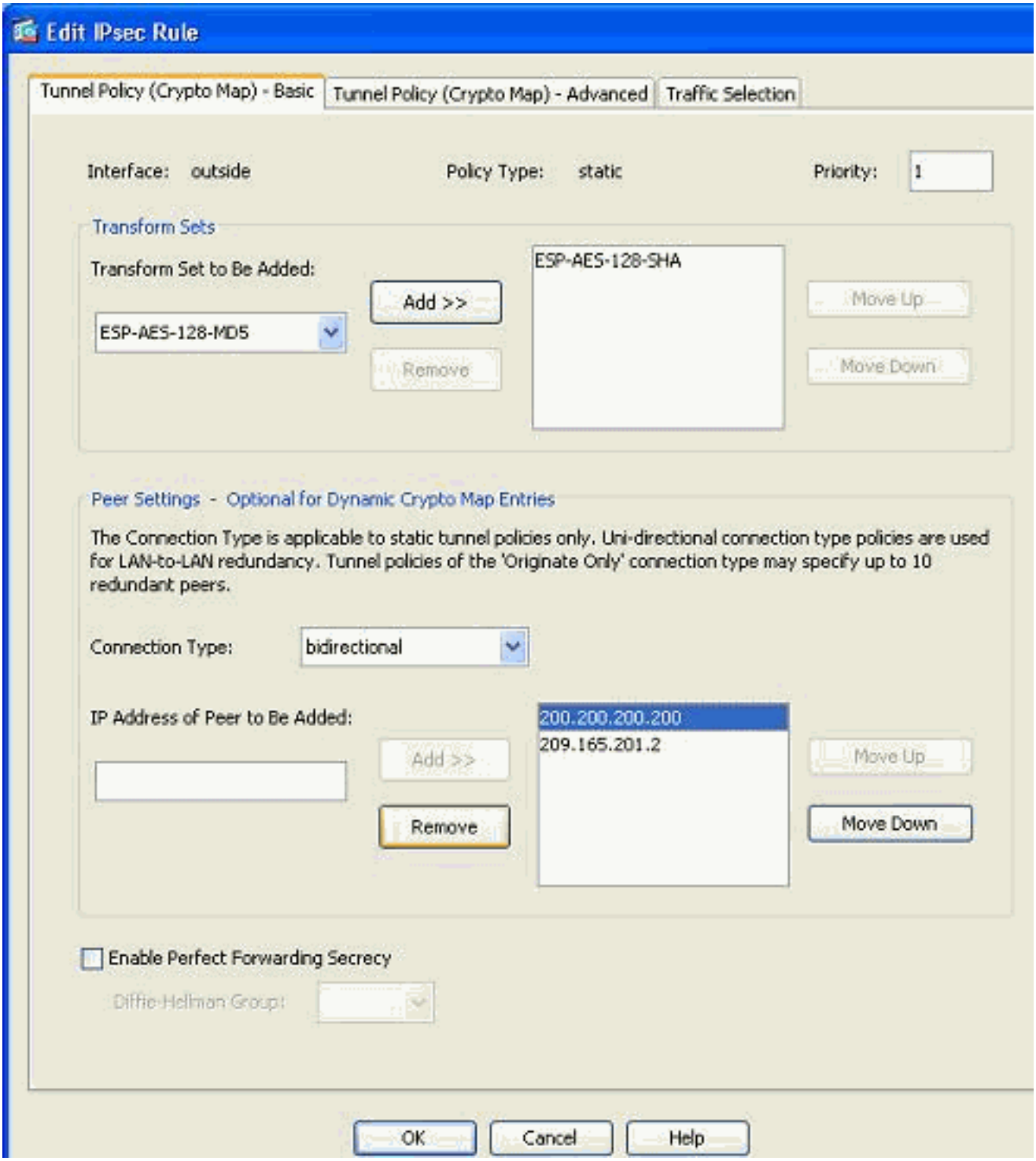
Complete estos pasos:

1. Van a la *configuración > al VPN de sitio a sitio > avanzaron > las correspondencias de criptografía*, después seleccionan la correspondencia de criptografía requerida y el tecleo *edita*.


La ventana de la *regla del IPSec del editar* aparece.
2. Bajo lengueta (básica) de la directiva del túnel, en el área de las configuraciones del par, especifique al nuevo par en la dirección IP del par para ser campo agregado. Entonces, haga click en
Add

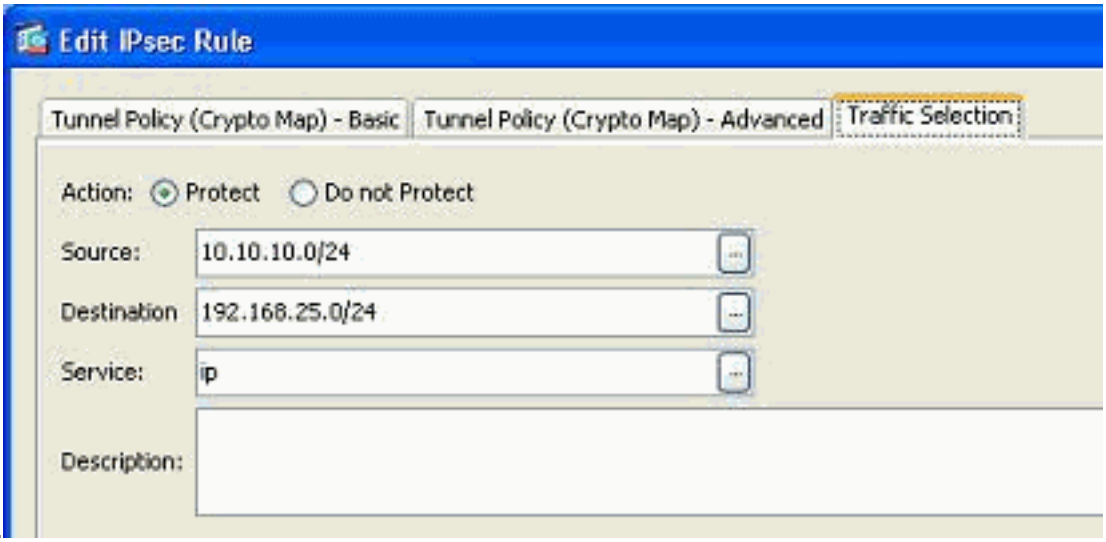


3. Seleccione el IP Address de Peer existente y el tecleo *quita* para conservar la nueva información de peer solamente. Haga clic en OK.



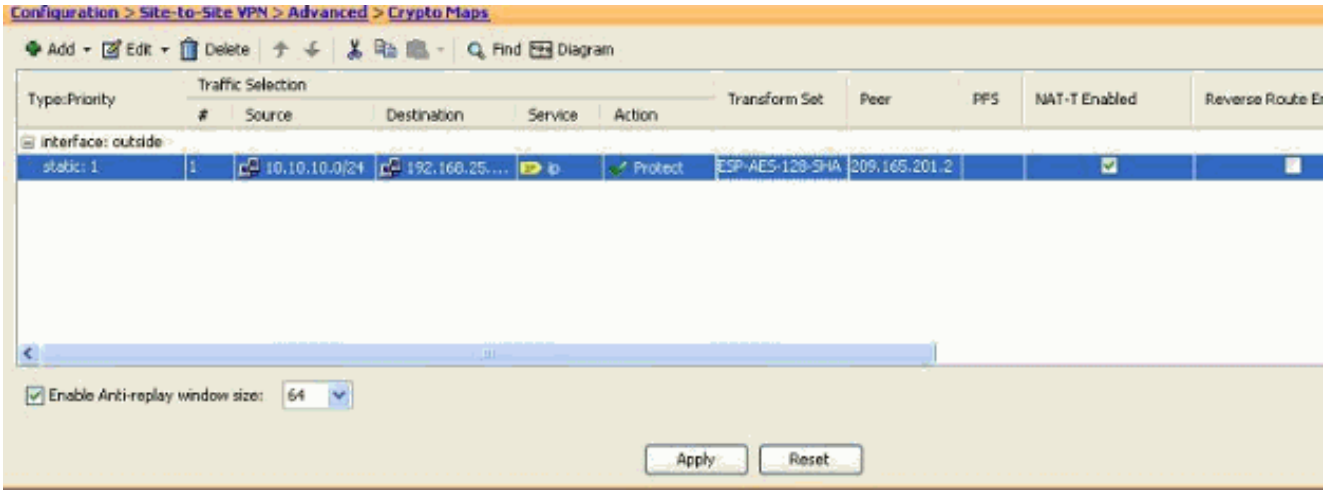
Nota: Después de que usted modifique la información de peer en la correspondencia de criptografía actual, el perfil de la conexión asociado a esta correspondencia de criptografía se borra inmediatamente en la ventana del ASDM.

4. Los detalles de las redes cifradas siguen siendo lo mismo. Si usted necesita modificar éstos, vaya a la lengueta de la *selección del*



tráfico.

5. Va a la *configuración > al VPN de sitio a sitio > avanzó > el* cristal de las *correspondencias de criptografía* para ver la correspondencia de criptografía modificada. Sin embargo, estos cambios no ocurren hasta que usted tecleo *se aplique*. Después de que usted tecleo *se aplique*, va a la *configuración > al VPN de sitio a sitio > avanzó > el* menú de los *grupos de túnel* para verificar si un grupo de túnel asociado está presente o no. Si sí, entonces un *perfil de la conexión* asociado será
creado.



Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- Utilice este comando de ver los parámetros de la asociación de seguridad específicos a un solo par:muestre la dirección IP crypto del <Peer del par IPSec sa >

Troubleshooting

Use esta sección para resolver problemas de configuración.

IKE Initiator unable to find policy: Test_ext de Intf, src: 172.16.1.103, dst: 10.1.4.251

Este error se visualiza en los mensajes del registro al intentar cambiar el VPN mira de un concentrador VPN al ASA.

Solución:

Éste puede ser un resultado de los pasos de la configuración inapropiada seguidos durante la migración. Asegúrese de que el atascamiento crypto a la interfaz esté quitado antes de que usted agregue a un nuevo par. También, aseegurese que usted utilizó la dirección IP del par en el grupo de túnel, pero no el nombre.

Información Relacionada

- Sitio para localizar (L2L) el VPN con el ASA
- La mayoría de los problemas comunes VPN
- Página de soporte técnico ASA
- Soporte Técnico y Documentación - Cisco Systems